

SPのトラストアンカーの確認と必要なCA証明書の導入(How to check your trust anchor and install a required CA certificate)

 [English version is here.](#)

現在メタデータリポジトリのサーバ証明書はSHA-1証明書を使用していますが、今後SHA-2証明書に移行する予定です。SHA-2証明書への移行時にはOSやパッケージのバージョンによって、必要となるCA証明書が入っていない可能性があり、確認・導入の作業が発生する見込みです。

すでにSPを構築済み・運用中の方は、以下の手順に従って利用しているOS、パッケージのバージョンをご確認ください。

これからSP構築される方は構築段階で確認・導入しておくことで将来行うべき作業が不要となりますので、今回を機会にご対応ください。

- [CentOS 6の場合](#)
- [CentOS 5の場合](#)
- [How to check your trust anchor and install a required CA certificate\(English Version\)](#)

CentOS 6の場合

- ca-certificatesパッケージが ca-certificates-2013.1.94-65.0.el6.noarch.rpm およびそれ以降であることを確認してください。

```
# rpm -q ca-certificates
```

- 異なる場合は最新版にアップデートしてください。

```
# yum update ca-certificates
```

- 以下のようにwgetコマンドで <https://attrviewer20.gakunin.nii.ac.jp/> にアクセスし、正常にページを取得できることを確認してください。

```
# wget https://attrviewer20.gakunin.nii.ac.jp/
--2015-03-18 14:36:25-- https://attrviewer20.gakunin.nii.ac.jp/
Resolving attrviewer20.gakunin.nii.ac.jp... 157.1.65.37
Connecting to attrviewer20.gakunin.nii.ac.jp|157.1.65.37|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5133 (5.0K) [text/html]
Saving to: `index.html'

100%[=====>] 5,133      --.-K/s   in 0s

2015-03-18 14:36:25 (46.6 MB/s) - `index.html' saved [5133/5133]
```

CentOS 5の場合

 すでに本ページの [CA証明書の導入方法\(openssl-0.9.8e-34.el5_11より前のバージョンの場合\)](#) でSECOMのSHA-2 CA証明書を導入済みの場合は、opensslパッケージをアップデート後に /etc/pki/tls/certs/ca-bundle.crt.rpmnew というファイルを /etc/pki/tls/certs/ca-bundle.crt へリネームし、opensslパッケージ提供のトラストアンカー(ca-bundle.crt)を利用してください。正しくアップデートされたことは、以下に記載のwgetコマンドを使った方法で確認してください。

- opensslパッケージが openssl-0.9.8e-34.el5_11 およびそれ以降であることを確認してください。

```
# rpm -q openssl
```

- 異なる場合は最新版にアップデートしてください。

```
# yum update openssl
```

- 以下のようにwgetコマンドで <https://attrviewer20.gakunin.nii.ac.jp/> にアクセスし、正常にページを取得できることを確認してください。

```
# wget https://attrviewer20.gakunin.nii.ac.jp/
--2015-03-18 14:36:25-- https://attrviewer20.gakunin.nii.ac.jp/
Resolving attrviewer20.gakunin.nii.ac.jp... 157.1.65.37
Connecting to attrviewer20.gakunin.nii.ac.jp|157.1.65.37|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5133 (5.0K) [text/html]
Saving to: `index.html'

100%[=====>] 5,133      --.-K/s   in 0s

2015-03-18 14:36:25 (46.6 MB/s) - `index.html' saved [5133/5133]
```

CA証明書の導入方法(openssl-0.9.8e-34.el5_11より前のバージョンの場合)



CentOS 5ではopensslパッケージに含まれる ca-bundle.crt が openssl-0.9.8e-34.el5_11 にて更新されました。このパッケージへアップデートすることで、本手順を用いることなく必要なCA証明書の導入ができるようになりました。パッケージの詳細は以下をご参照ください。

- [CentOS-announce] CEEA-2015:0958 CentOS 5 openssl Enhancement Update
<http://lists.centos.org/pipermail/centos-announce/2015-May/021134.html>

SPのトラストアンカーとしてSECOMのCA証明書を導入する手順としては不要となりますが、個別にCA証明書を導入する要件がある場合に利用可能ですので情報として残しています。

CentOS 5上で稼働するSPのトラストアンカーにSECOMのSHA-2 CA証明書を導入する手順について記載します。

証明書が導入されていないことの確認

以下のようにwgetコマンドで <https://attrviewer20.gakunin.nii.ac.jp/> にアクセスし、証明書のエラーとなることを確認します。

```
# wget https://attrviewer20.gakunin.nii.ac.jp/
--2015-03-18 14:32:33-- https://attrviewer20.gakunin.nii.ac.jp/
Resolving attrviewer20.gakunin.nii.ac.jp... 157.1.65.37
Connecting to attrviewer20.gakunin.nii.ac.jp|157.1.65.37|:443... connected.
ERROR: cannot verify attrviewer20.gakunin.nii.ac.jp's certificate, issued by `/C=JP/L=Academe/O=National Institute of Informatics/CN=NII Open Domain CA - G4':
  Unable to locally verify the issuer's authority.
To connect to attrviewer20.gakunin.nii.ac.jp insecurely, use `--no-check-certificate'.
Unable to establish SSL connection.
```

証明書の導入

- <https://repository.secomtrust.net/SC-Root2/index.html>からSecurity Communication Root CA2証明書をダウンロードします。ダウンロードしたファイルのファイル名は SCRoot2ca.cer とします。

- ダウンロードしたファイルはバイナリ形式のため、以下のコマンドでテキスト形式に変換します。

```
# openssl x509 -inform DER -in SCRoot2ca.cer -outform PEM -out scrootca2.txt
```

- 以下のコマンドでテキスト形式に変換したファイルのフィンガープリントが以下の例と一致することを確認します。

```
# openssl x509 -in scrootca2.txt -noout -fingerprint -sha256
SHA256 Fingerprint=51:3B:2C:EC:B8:10:D4:CD:E5:DD:85:39:1A:DF:C6:C2:DD:60:D8:7B:B7:36:D2:B5:21:48:4A:A4:7A:0E:BE:F6

# openssl x509 -in scrootca2.txt -noout -fingerprint -md5
MD5 Fingerprint=6C:39:7D:A4:0E:55:59:B2:3F:D6:41:B1:12:50:DE:43

# openssl x509 -in scrootca2.txt -noout -fingerprint -sha1
SHA1 Fingerprint=5F:3B:8C:F2:F8:10:B3:7D:78:B4:CE:EC:19:19:C3:73:34:B9:C7:74
```

- ・ 既存のトラストアンカーをバックアップします。

```
# cp /etc/pki/tls/certs/ca-bundle.crt /etc/pki/tls/certs/ca-bundle.crt.backup
```

- ・ 既存のトラストアンカーを新規ファイルにコピーします。

```
# cp /etc/pki/tls/certs/ca-bundle.crt ca-bundle.crt.new
```

- ・ 新規ファイルにSECOMのSHA-2 CA証明書を追加します。

```
# openssl x509 -in scrootca2.txt -noout -text >> ca-bundle.crt.new
# cat scrootca2.txt >> ca-bundle.crt.new
```

- ・ 証明書を追加したトラストアンカーを既存のトラストアンカーと置き換えます。

```
# cp ca-bundle.crt.new /etc/pki/tls/certs/ca-bundle.crt
# chown root:root /etc/pki/tls/certs/ca-bundle.crt
# chmod 644 /etc/pki/tls/certs/ca-bundle.crt
```

証明書が導入されたことの確認

以下のようにwgetコマンドで <https://attrviewer20.gakunin.nii.ac.jp/> にアクセスし、正常にページを取得できることを確認します。

```
# wget https://attrviewer20.gakunin.nii.ac.jp/
--2015-03-18 14:36:25-- https://attrviewer20.gakunin.nii.ac.jp/
Resolving attrviewer20.gakunin.nii.ac.jp... 157.1.65.37
Connecting to attrviewer20.gakunin.nii.ac.jp|157.1.65.37|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5133 (5.0K) [text/html]
Saving to: `index.html'

100%[=====>] 5,133      --.-K/s   in 0s

2015-03-18 14:36:25 (46.6 MB/s) - `index.html' saved [5133/5133]
```

How to check your trust anchor and install a required CA certificate(English Version)

If your OS is 'CentOS 6':

- ・ Please check whether your 'ca-certificates' package is either 'ca-certificates-2013.1.94-65.0.el6.noarch.rpm' or a newer version.

```
# rpm -q ca-certificates
```

- ・ If it is not, please update it to the latest version.

```
# yum update ca-certificates
```

- Please access to <https://attrviewer20.gakunin.nii.ac.jp/> by using a wget command, and check that you are acquiring the page correctly (please refer to below):

```
# wget https://attrviewer20.gakunin.nii.ac.jp/
--2015-03-18 14:36:25-- https://attrviewer20.gakunin.nii.ac.jp/
Resolving attrviewer20.gakunin.nii.ac.jp... 157.1.65.37
Connecting to attrviewer20.gakunin.nii.ac.jp|157.1.65.37|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5133 (5.0K) [text/html]
Saving to: `index.html'

100%[=====>] 5,133      --.-K/s   in 0s

2015-03-18 14:36:25 (46.6 MB/s) - `index.html' saved [5133/5133]
```

If your OS is 'CentOS 5':

- Please check whether your 'openssl' package is either 'openssl-0.9.8e-34.el5_11' or a newer version.

```
# rpm -q openssl
```

- If it is not, please update it to the latest version.

```
# yum update openssl
```

- Please access to <https://attrviewer20.gakunin.nii.ac.jp/> by using a wget command, and check that you are acquiring the page correctly (please refer to below):

```
# wget https://attrviewer20.gakunin.nii.ac.jp/
--2015-03-18 14:36:25-- https://attrviewer20.gakunin.nii.ac.jp/
Resolving attrviewer20.gakunin.nii.ac.jp... 157.1.65.37
Connecting to attrviewer20.gakunin.nii.ac.jp|157.1.65.37|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5133 (5.0K) [text/html]
Saving to: `index.html'

100%[=====>] 5,133      --.-K/s   in 0s

2015-03-18 14:36:25 (46.6 MB/s) - `index.html' saved [5133/5133]
```